UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/767,842	01/30/2004	Yasuyuki Higashiura	040033	4101

23850 7590 02/05/2008

KRATZ, QUINTOS & HANSON, LLP
1420 K Street, N.W.
Suite 400
WASHINGTON, DC 20005

EXAMINER	
KIM, JUNG W	
ART UNIT	**PAPER NUMBER**
2132	

MAIL DATE	DELIVERY MODE
02/05/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/767,842	HIGASHIURA ET AL.	
	Examiner	Art Unit	
	Jung Kim	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 November 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This Office action is in response to the amendment filed on 11/13/07.

2. Claims 1-21 are pending.

Response to Amendment

3. The 112/2nd paragraph rejections to claims 3-5, 7-10, 12, 14, 15 and 18-21 are withdrawn as the amendment overcomes the 112/2nd paragraph rejections.

Response to Arguments

4. Applicant's prior art arguments with respect to the amended claims have been considered but are moot in view of the new ground(s) of rejection.

Claim Objections

5. Claims 12, 14 and 14 are objected to because of the following informalities:

   a. On line 4 of claim 12, replace "created at access to the public key-based after verifying" with –created at access to the public key-based electronic signature after verifying--.

   b. The limitations of claims 14 and 15 are identical.

Appropriate correction is required.

Claim Rejections - 35 USC § 103

6. Claims 1-5 and 11-15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bacha et al. USPN 6,950,943 (hereinafter Bacha).

7. As per claims 1, 3 and 4, Bacha discloses an electronic data storage system comprising:

c. a file device for storing at least electronic data (fig. 2, reference no. 204); and

d. a data processing unit which generates a first check code for detecting falsification of said electronic data and a second check code for detecting falsification of a public key-based electronic signature using a secret encryption method and/or an encryption key when the electronic data is registered (Col. 5:60-65; 6:12-15; 6:41-45; 7:1-3), stores said electronic data, said public key-based electronic signature, and said first and second check codes into said file device (7:9-12), respectively verifies the validity of said stored electronic data and said electronic signature using said first and second check codes when said electronic data is output, and then accesses said electronic data and said electronic signature when said validity is confirmed; (7:12-25; 8:15-54)

e. wherein the data processing unit generates the first and second check codes by a method unique to the system; (private/public key pair is unique to the repository service)

f. further comprising a step of outputting said electronic data, the public key-based electronic signature and a second key-based electronic signature created at access to the public key-based electronic signature or the electronic data after verifying the validity of said electronic data and said electronic signature. (7:12-25; 8:15-34 [the notarized signature includes the originator's signature and the notary's signature of the originator's signature (6:59-63)])

Bacha does not disclose the data processing unit verifies the validity of the stored electronic data and the electronic signature by creating a third check code from the electronic data and a fourth check code from the electronic signature by the method unique to the system, and comparing the stored first check code with the third check code and the stored second check code with the fourth check code. However, Bacha discloses it is well known in the art to compute a signature by first computing a digest of a data element, then signing the digest. (5:66-6:15) As known in the art, creating a digest before signing the digest results in a smaller signature value, which enables smaller storage requirements. Furthermore, authentication of any signed (private key) digest requires 1) using the corresponding public key to decrypt the signed digest, and 2) hashing the original data element to create a second digest, then comparing the decrypted digest with the second digest as known to one of ordinary skill in the art. Hence, this teaching applied to the other portions of Bacha suggest verifying the validity of the stored electronic data and the electronic signature by creating a third check code from the electronic data and a fourth check code from the electronic signature by the method unique to the system, and comparing the stored first check code with the third

check code and the stored second check code with the fourth check code. One would be motivated to do so to provide smaller storage requirements.

Finally, although Bacha does not expressly disclose wherein the first check code is attached to the electronic data and the second check code is attached to the electronic signature, it is notoriously well known in the art to attach the integrity check value of a data element to the data element. For example, in X.509 protocol, issuer signatures for public key certificates are appended to the certificate. This ensures that the signature is linked to the certificate to easily verify the certificate. Official notice of this teaching is taken. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made wherein the first check code is attached to the electronic data and the second check code is attached to the electronic signature. One would be motivated to do so to easily locate the first check code for the data and the second check code for the signature. The aforementioned cover the limitations of claims 1, 3 and 4.

8. As per claims 2 and 5, Bacha discloses an electronic data storage system comprising:

g. a file device for storing at least electronic data (fig. 2, reference no. 204); and

h. a data processing unit which generates a check code for detecting falsification of a public key-based electronic signature using a secret encryption method and/or an encryption key when the electronic data is registered (Col.

5:60-65; 6:12-15; 6:41-45; 7:1-3), stores said electronic data, said public key-based electronic signature, and the falsification check codes into said file device (7:9-12), verifies the validity of said electronic signature using the check code (7:12-25); verifies the validity of said electronic data using said electronic signature when said electronic data is output (8:15-30), and then accesses said electronic data and said electronic signature when said validity is confirmed; (8:31-54)

i. wherein the data processing unit generates the check code; (private/public key pair is unique to the repository service)

j. further comprising a step of outputting said electronic data, the public key-based electronic signature and a second key-based electronic signature created at access to the public key-based electronic signature after verifying the validity of said electronic data and said electronic signature. (7:12-25; 8:15-34 [the notarized signature includes the originator's signature and the notary's signature of the originator's signature (6:59-63)])

Bacha does not disclose the data processing unit verifies the validity of the stored electronic data by creating a second check code from the electronic signature by the method unique to the system, and comparing the stored check code with the second check code. However, Bacha discloses it is well known in the art to compute a signature by first computing a digest of a data element, then signing the digest. (5:66-6:15) As known in the art, creating a digest before signing the digest results in a smaller signature value, which enables smaller storage requirements. Furthermore,

authentication of any signed (private key) digest requires 1) using the corresponding public key to decrypt the signed digest, and 2) hashing the original data element to create a second digest, then comparing the decrypted digest with the second digest as known to one of ordinary skill in the art. Hence, this teaching applied to the other portions of Bacha suggest verifying the validity of the stored electronic data by creating a second check code from the electronic signature by the method unique to the system, and comparing the stored check code with the second check code. One would be motivated to do so to provide smaller storage requirements.

Finally, although Bacha does not expressly disclose wherein the first check code is attached to the electronic signature, it is notoriously well known in the art to attach the integrity check value of a data element to the data element. For example, in X.509 protocol, issuer signatures for public key certificates are appended to the certificate. This ensures that the signature is linked to the certificate to easily verify the certificate. Official notice of this teaching is taken. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made wherein the first check code is attached to the electronic signature. One would be motivated to do so to easily locate the signature's check code. The aforementioned cover the limitations of claims 2 and 5.

9. As per claims 11-15, they are claims corresponding to claims 1-5, and they do not teach or define above the information claimed in claims 1-5. Therefore, claims 11-15 are rejected as being unpatentable over Bacha for the same reasons set forth in the rejections of claims 1-5.

10. Claims 6-10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bacha in view of Bisbee et al. USPN 5,748,738 (hereinafter Bisbee).

11. As per claims 6-10, the rejections of claims 1-5 under 35 USC 103(a) as being unpatentable over Bacha are incorporated herein. Bacha does not expressly disclose, wherein said data processing unit stores a certificate of the public key with which said electronic signature was created, simultaneously along with said electronic signature into the file device, when said electronic signature is created; wherein said data processing unit stores or outputs the expiration information of said public key certificate simultaneously; wherein said data processing unit stores a certificate of the public key with which said electronic signature is created, simultaneously along with said electronic signature into the file device, when said electronic signature is created; wherein said data processing unit stores or outputs the expiration information of said public key certificate simultaneously; wherein said data processing unit creates a pair of said public key and said secret key according to a request for key creation, issues a request of issuing a public key certificate to a CA office, acquires a public key certificate, and stores said acquired public key certificate in said file device. Bisbee discloses a system and method for electronic storage of authenticated documents, wherein a Certificate authority issues a public key certificate to various subscribers to generate public key signatures, wherein the certificates are in accordance with X.509, wherein the certificates include an expiration period field to indicate the expiration of the certificate;

wherein a first digital signature is generated from an electronic document using a first private key from a first certificate, and the first digital signature and first certificate are attached to the electronic document; whereupon a second digital signature is generated from the electronic document using a second private key from a second certificate, and the second digital signature and second certificate are attached to the electronic document then stored in an Authentication Center once the first digital signature is validated. (5:15-55; 7:15-22; 9:27-10:7; 10:50-64) It would be obvious to one of ordinary skill in the art at the time the invention was made for the invention of Bacha to include the features wherein said data processing unit stores a certificate of the public key with which said electronic signature was created, simultaneously along with said electronic signature into the file device, when said electronic signature is created; wherein said data processing unit stores or outputs the expiration information of said public key certificate simultaneously; wherein said data processing unit stores a certificate of the public key with which said electronic signature is created, simultaneously along with said electronic signature into the file device, when said electronic signature is created; wherein said data processing unit stores or outputs the expiration information of said public key certificate simultaneously; wherein said data processing unit creates a pair of said public key and said secret key according to a request for key creation, issues a request of issuing a public key certificate to a CA office, acquires a public key certificate, and stores said acquired public key certificate in said file device. One would be motivated to do so to provide simple and efficient means to provide the certified public key used to verify the public key signature of the electronic

document as known to one of ordinary skill in the art and as taught by Bisbee. Col. 2:64-3:11. The aforementioned cover the limitations of claims 6-10.

12. As per claims 16-21, they are claims corresponding to claims 6-10, and they do not teach or define above the information claimed in claims 6-10. Therefore, claims 16-21 are rejected as being unpatentable over Bacha in view of Bisbee for the same reasons set forth in the rejections of claims 6-10.

Communications Inquiry

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W. Kim whose telephone number is 571-272-3804. The examiner can normally be reached on M-F 9:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Jung Kim/
Examiner AU 2132

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100